2006

Waging war through the Internet; America is far more vulnerable to terrorists who hack systems than missions to blow things up

Waging war through the Internet / America is far more vulnerable to terrorists who hack systems than missions to blow things up

John Arquilla
Published 4:00 am, Sunday, January 15, 2006

Over the past four years, huge efforts have been made to keep al Qaeda and other terrorist organizations from acquiring weapons of mass destruction, but too little attention has been paid to threats from cyberspace-based weapons of "mass disruption" capable of crippling the United States' communications, energy and transportation infrastructures.

Imagine an enemy able to knock out the power in some sizable chunk of the country by means of fast-spreading viruses inserted into our computer systems. Or think of an adversary who can gain remote access to and then crash highly automated controls that run many sensitive operations, from hydroelectric dams to gas and oil pipelines and robotic chemical plants.

This concern is not just theoretical. There have been real instances of these types of attack already.

For example, information systems of a major hydroelectric dam in this country were briefly intruded upon. In Australia, a disgruntled man gained access to a wastewater treatment plant's automated control system and caused it to release large amounts of untreated sewage.

In a case that I investigated personally some years ago, a skillful hacker gained administrator-level control of a Department of Energy nuclear research facility's information systems and could have done enormous damage. Happy enough with his exploit of gaining access, the hacker left without doing much harm.

We got lucky at that nuclear research facility. But the point is that all sorts of cyber attacks are possible -- and they're coming.

Those of us who are watching see the signs in the continuing and intensive mapping of such targets by covert operatives.

Department of Defense systems have come under sustained cyber attacks, too. An early series of such intrusions, back-hacked by us as far as a computer server in Moscow, came to be known as "Moonlight Maze."

More recently, similar probing by hackers who seem to be Chinese is bedeviling us in a cyber campaign known as "Titan Rain."

Both Moonlight Maze and Titan Rain remain classified matters. Moonlight Maze, sometimes called "M2," began in the late 1990s, when we first detected a series of systematic intrusions into Pentagon systems.

The amazing part of it is that the intruders retained an ability to keep coming back into our systems, even while we were actively trying to block them. Often, there was a cyber thrust-and-parry going on in real time, as our cyber warriors tried both to block and to back-hack them, with varying degrees of success.

Like Neo vs. Agent Smith in "The Matrix," but without all the special effects, M2 offered an example of the kind of fighting in the virtual domain that cyber-punk pioneer William Gibson envisioned over 20 years ago in his classic "Neuromancer."

Where M2 appeared to have a Russian connection, Titan Rain -- which is going on right now -- seems linked to China, home to some of the world's most skillful hackers. They have been mounting cyber attacks on critical Taiwanese information infrastructures for years, as well as on economic targets such as the stock exchange in Taipei.

Like M2, Titan Rain also features deep intrusions into our sensitive military and scientific systems, mapping our information architectures and apparently accessing information about weapons and other systems.

Even in the absence of a serious cyber-terror campaign orchestrated by a specific group, the claims paid by insurers for cyber disruptions each year already exceed $40 billion. Since insurers paid about the same amount in insured losses resulting from the Sept. 11, 2001, attacks, it can be said that cyber attacks cost us, financially -- but not in loss of life -- the equivalent of a Sept. 11 every year.

Of course, these damages pale next to the dire consequences of a terror network coming into possession of a nuclear warhead. But it is highly unlikely that this will happen, because the nuclear weapons development process is extremely costly and complicated, and the alternate path, purchasing such devices, is fraught with potentially fatal security risks for the terrorists.

A capacity for cyber terror, on the other hand, is easily within reach for al Qaeda, other terror networks and rogue nations. Even individuals can play important roles as combatants in the virtual realm, since the world of computer viruses, worms and Trojan horses is truly one of remote, push-button warfare. All who have the requisite knowledge can soon be "clicking for their cause."

Many already possess this know-how, and the number of cyber warriors worldwide is growing swiftly. As to al Qaeda, it is thought to have sent at least one operative to the United States to learn computer science, although many more of the terror network's budding alpha geeks were given instruction elsewhere before Sept. 11.

Despite knowing of al Qaeda's long-standing interest in cyber terror, we have been a bit dismissive of this burgeoning threat. In part, that's because we doubt terrorists will focus on using computers to attack computer systems, believing instead that "real terrorists" want to kill people and blow things up far more than they want to cause data crashes.

From a purely psychological point of view, this idea makes sense, as traditional terrorists have been leg-breakers, for the most part. But over the past four years, we have made it very hard for al Qaeda to mount new attacks within the United States.

So, if Osama bin Laden wants to pursue his goal of attacking our economy, disruptive cyber-terror strikes via the Internet are likely to be an increasingly important element in his offensive.

The other reason for our being somewhat complacent about cyber terror derives from overconfidence in our defensive capabilities.

We believe that firewalls and other security tools really can protect us. There is a whole computer security industry out there, working hard every day to convince us that the virtual world can be made a safe place to do business. American companies and consumers do spend quite lavishly on this kind of security, and the Pentagon's expenditures on cyber defenses dwarf the private sector's.

Yet a goodly portion of what is paid out for cyber security is wasted. The big problem is that firewalls are generally effective only at thwarting attacks that employ already known tools and methods. Something entirely new, or a rejiggering of an older strain of a computer virus, will sail right past most firewalls, causing huge damage.

It's a situation like that caused by European explorers beginning in the 16th century. They traveled the world and brought their germs, against which the vast majority of indigenous peoples had no immunity. The result was a kind of running biological Holocaust.

If we remain firewall-dependent, sooner or later we'll find ourselves in the same situation, struck by a series of computer viruses and worms that move right through the permeable membranes of our security systems.

But there are some things we can do before al Qaeda tries to conquer us via cyberspace. The most important defensive measure we can take is to use strong encryption.

With little cost or loss of time or convenience, we could make it impossible for cyber terrorists to gain access to our systems, or to exploit them if they did gain entry. They simply wouldn't know what they were looking at, or how to find their way around a system

they had hacked into.

Sadly, the U.S. government -- during both Democratic and Republican administrations -- spent many years fighting to keep strong encryption out of the hands of the American people.

That was most probably done so that U.S. law enforcement and intelligence agencies could retain the ability to engage in cyber snooping. But all it really did was create a situation in which criminals and terrorists now have good encryption while most of us still do not.

Today, it is legal for individuals to employ codes with unbreakably long lengths, but few people use them. Less than 10 percent of Internet traffic is encrypted at all. This is true of the military as well, where strong encryption is still seen as too much of an inconvenience.

Even if we never get our cyber defensive act together, there is something we can do offensively: detect and hack into the terrorists' own systems. Some of this goes on now, but far more must be done. Of the roughly $40 billion spent each year on intelligence, only a relative thimbleful goes to Web- and Net-based activities. This needs to change.

Given that the terrorists are doing a lot to secure their own systems, we should recruit more of the world's master hackers to our cause. They'll give us our best chance of cracking even strongly encrypted terrorist communications.

The best part of making this move is that we'll learn far more about the terrorists than we have ever known before. This will give us a real chance of winning the war on terror, while at the same time reducing the intrusions on Americans' privacy.

In the meantime, get ready. The terrorists are preparing to mount cyberspace-based attacks, and we are ill prepared to deal with them.

We know from the capture of Khalid Sheik Mohammed early on in the war on terror and the more recent capture of Abu Musab al Zarqawi's laptop (but not of the man himself) that al Qaeda is a sophisticated user of advanced information technology. From other sources we have learned of the terror network's intent to launch a cyber-terror campaign. So, the clock is ticking toward a showdown with these weapons of mass disruption.

Let's hope our leaders have the wit and grit to secure our information systems, and to realize that, although our enemies may dwell in caves, they do much of their work in cyberspace. This, if we're smart about it, will turn out to be a fatal weakness of theirs -- one just begging to be exploited.